IN THE CLAIMS

Please enter the following clarifying claim amendments:

1. (currently amended) A method for cryptographically processing data, said method comprising:

receiving a ~~plurality of data segments~~ **first data segment**;

~~selecting a set of encryption information for a current data segment to be encrypted based on data contained in a predetermined portion of the current data segment;~~

identifying at least two portions of the first data segment, including a first portion and a second portion;

generating a first hash value from the first portion of the first data segment;

identifying a first encryption scheme from among a plurality of encryption schemes, the first encryption scheme being identified by the first hash value corresponding to the first portion of the first data segment; and

encrypting**, with a computer processor, at least a part of** the ~~current~~ **first** data segment using the ~~set of encryption information selected for the current data segment~~ **the first encryption scheme**~~; and~~

~~repeating said selecting and said encrypting for subsequent data segments~~.

Claims 2-4. (canceled)

5. (currently amended) The method of claim ~~3~~ **1**, further comprising:

providing an encryption table ~~containing~~ **for selecting an encryption scheme from a hash value, the encryption table comprising**:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a ~~generate~~ **potential hash** value **corresponding to the first portion of the first data segment**.

6. (canceled)

7. (currently amended) The method of claim **~~6~~ 1**, **~~wherein said receiving comprises~~ further comprising**:

receiving a data stream comprising the first data segment and a plurality of additional data segments, each of the first data segment and the plurality additional data segments corresponding to a data packet of the data stream

~~receiving a data stream including a plurality of data packets, each data packet corresponding to a data segment~~.

8. (currently amended) The method of claim **~~7~~ 1**, wherein the first **~~predetermined~~** portion contains data for a first protocol layer, and the second **~~predetermined~~** portion contains data for a second protocol layer**~~, wherein the first protocol layer is lower than the second protocol layer~~**.

9. (currently amended) The method of claim **~~7~~ 1**, wherein the first **~~predetermined~~** portion is an Internet Protocol (IP) header of the **~~data packet~~ first data segment**.

10. (currently amended) The method of claim 9, wherein the second **~~predetermined~~** portion is **~~either~~** one of:

a selected portion of a data field of the data packet;

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

Claims 11-12. (canceled)

13. (currently amended) The method of claim **~~6~~ 1**, **~~wherein said receiving comprises~~ further comprising**:

reading **~~the~~ a** plurality of data segments**, including the first data segment,** from corresponding sectors in a data storage device.

Claims 14-15. (canceled)

16. (currently amended) The method of claim ~~15~~ **103**, ~~**further comprising: encrypting**~~ **the third portion being** the remaining portion of the **current** data segment ~~**using the second set of encryption information**~~**, excluding the first portion and the second portion**.

17. (currently amended) The method of claim ~~**16**~~ **103**, further comprising:

~~**generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment**~~ **outputting an encrypted current data segment comprising the first portion remaining unencrypted, the second portion encrypted according to the first encryption scheme, and the third portion encrypted according to the second encryption scheme**.

18. (currently amended) The method of claim ~~**17**~~ **7**, further comprising:

encrypting the plurality of additional data segments; and

transmitting ~~**[[a]]**~~ **the resulting** plurality of encrypted data segments as a stream of encrypted data.

19. (currently amended) The method of claim ~~**17**~~ **13**, further comprising:

encrypting the plurality of data segments; and

storing ~~**[[a]]**~~ **the resulting** plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device.

20. (currently amended) The method of claim 17, further comprising:

receiving ~~**the encrypted data including a plurality of encrypted data segments**~~ **the encrypted current data segment corresponding to the current data segment**;

~~**selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment;**~~

~~decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment;~~

~~selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion; and~~

~~decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment~~

selecting a first decryption scheme and a second decryption scheme;

decrypting the encrypted current data segment to recover the current data segment by applying a first decryption scheme to the encrypted second predetermined portion and applying a second decryption scheme to the encrypted third predetermined portion.

Claims 21-24. (canceled)

25. (currently amended) A method for cryptographically processing data, said method comprising:

receiving a ~~plurality of~~ **first** encrypted data segment~~[[s]], each of the encrypted data segments having a predetermined portion~~;

~~selecting a set of encryption information for a current encrypted data segment to be decrypted based on data contained in the predetermined portion of the current encrypted data segment;~~

identifying at least two portions of the first encrypted data segment, including a first portion and a second portion;

generating a first hash value from the first portion of the first encrypted data segment;

identifying a first encryption scheme from among a plurality of encryption schemes, the first encryption scheme being identified by the first hash value corresponding to the first portion of the first encrypted data segment; and

decrypting**, with a computer processor, at least a part of** the ~~current~~ **first** encrypted data segment using the ~~encryption information selected for the current encrypted data segment~~ **first encryption scheme; and**

~~repeating said selecting and said decrypting for subsequent encrypted data segments~~.

Claims 26-27. (canceled)

28. (currently amended) The method of claim ~~27~~ **25**, further comprising:

providing an encryption table **for selecting an encryption scheme from a hash value**, the encryption table ~~containing~~ **comprising**:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a ~~generated~~ **potential hash** value **corresponding to the first portion of the first encrypted data segment**.

29. (canceled)

30. (currently amended) The method of claim ~~29~~ **25**, ~~wherein said receiving comprises~~ **further comprising**:

receiving an encrypted data stream comprising the first encrypted data segment and a plurality of additional encrypted data segments, each of the first encrypted data segment and the plurality additional encrypted data segments corresponding to a data packet of the encrypted data stream

~~receiving an encrypted data stream including a plurality of encrypted data packets, each encrypted data packet corresponding to an encrypted data segment~~.

31. (currently amended) The method of claim ~~30~~ **25**, wherein the first ~~predetermined~~ portion **of the first encrypted data segment** contains data for a first protocol layer, and the second ~~predetermined~~ portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

32. (currently amended) The method of claim ~~30~~ **31**, ~~wherein~~ the first ~~predetermined~~ portion ~~is~~ **of the first encrypted data segment being** an Internet Protocol (IP) header of the ~~data packet~~ **first encrypted data segment**.

33. (currently amended) The method of claim 32, ~~wherein~~ the second ~~predetermined~~ portion ~~is either~~ **of the first encrypted data segment being** one of:

a selected portion of a data field of the data packet;

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

Claims 34-35. (canceled)

36. (currently amended) The method of claim ~~29~~ **25**, ~~wherein said receiving comprises~~ **further comprising**:

reading ~~the~~ **a** plurality of encrypted data segments**, including the first data segment,** from corresponding sectors in a data storage device.

37. (currently amended) The method of claim 36, ~~wherein~~ the first ~~predetermined~~ portion ~~is~~ **of the first encrypted data segment being** a first selected portion in a sector ~~in a~~ **of the** data storage device, and the second ~~predetermined~~ portion ~~is~~ **being** a second selected portion in the sector.

Claims 38-39. (canceled)

40. (currently amended) An apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive ~~data including a plurality of data segments~~ **a data segment**;

~~an encryption module adapted to encrypt each data segment;~~

a controller coupled to said input buffer ~~and said encryption module~~, said controller being adapted to **generate a first hash value from a first portion of the data segment and to dynamically** select a ~~set of encryption information for a current data segment to be encrypted based on data contained in a predetermined portion of the current data segment~~

first encryption scheme from a plurality of encryption schemes, each encryption scheme comprising an encryption algorithm and an encryption key, and the first encryption scheme corresponding to the first hash value;

an encryption module coupled to the controller and configured to utilize a computer processor to encrypt a second portion of the data segment using the first encryption scheme; and

an output buffer coupled to ~~said controller and~~ said encryption module, said output buffer being adapted to output ~~encrypted data including a plurality of encrypted data segments~~ **encrypted data corresponding to the data segment**.

41. (currently amended) The apparatus of claim 40, **the input buffer being further configured to receive a plurality of additional data segments, and the encryption module being further configured to encrypt the plurality of additional data segments,** wherein said controller changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each **of the plurality of additional** data segment**s**.

42. (currently amended) The apparatus of claim 40, wherein said encryption module comprises:

a plurality of encryption engines, each encryption engine corresponding to a ~~respective encryption algorithm different from each other~~ **distinct encryption algorithm**.

43. (currently amended) The apparatus of claim ~~40~~ **42**, wherein said encryption module further comprises:

a data buffer coupled to each of the plurality of encryption engines.

44. (currently amended) The apparatus of claim ~~40~~ **42**, wherein said controller comprises:

~~a data selector adapted to select a predetermined portion of each data segment;~~

~~an encryption selector coupled with said data selector, adapted to select a set of encryption information in accordance with data contained in the predetermined portion, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter; and~~

an encryption controller adapted to select and activate an encryption engine **for encrypting the second portion of the data segment** based on the ~~encryption information~~ **first encryption scheme corresponding to the first hash value**.

Claims 45-46. (canceled)

47. (currently amended) The apparatus of claim ~~45~~ **40**, ~~wherein said encryption~~ **the** controller ~~comprises~~ **comprising** an encryption table ~~containing~~ **for selecting an encryption scheme from a hash value, the encryption table comprising**:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a ~~generated~~ **potential hash** value **corresponding to the first portion of the data segment**.

48. (canceled)

49. (currently amended) The apparatus of claim ~~48~~ **40**, ~~wherein the plurality of data segments are data packets in a data stream~~ **the input buffer being further configured to receive a data stream comprising a plurality of data packets, the data segment being at least one of the data packets**.

50. (currently amended) The apparatus of claim 49, ~~wherein~~ the first ~~predetermined~~ portion ~~contains~~ **of the data segment comprising** data for a first protocol layer, and the second ~~predetermined~~ portion ~~contains~~ **comprising** data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

51. (currently amended) The apparatus of claim ~~49~~ **50**, ~~wherein~~ the first ~~predetermined~~ portion ~~is~~ **of the data segment being** an Internet Protocol (IP) header ~~of the data packet~~.

52. (currently amended) The apparatus of claim 51, ~~wherein~~ the second ~~predetermined~~ portion ~~is either~~ **of the data segment being** one of:

a selected portion of a data field of the data packet;

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

Claims 53-54. (canceled)

55. (currently amended) The method of claim ~~48~~ **40**, ~~wherein the plurality of data segments are sectors in a data storage device~~ **the input buffer being further configured to read the data segment from a sector of a data storage device**.

56. (currently amended) The apparatus of claim 55, ~~wherein~~ the first ~~predetermined~~ portion ~~is~~ **of the data segment being** a first selected portion in ~~[[a]]~~ **the** sector ~~in a~~ **of the** data storage device, and the second ~~predetermined~~ portion ~~is~~ **being** a second selected portion ~~in~~ **of** the sector.

57. (currently amended) The apparatus of claim ~~48~~ **109**, ~~wherein said~~ **the** controller ~~comprises~~ **further comprising**:

a first encryption table for **mapping a plurality of potential hash values to the plurality of encryption schemes, wherein the controller identifies** ~~selecting~~ the first ~~set of encryption information based on data contained in the first predetermined portion~~ **encryption scheme as corresponding to the first hash value in the first encryption table**; and

a second encryption table for **mapping a plurality of potential hash values to the plurality of encryption schemes, wherein the controller identifies** ~~selecting~~ the second ~~set of encryption information based on data contained in the second predetermined portion~~ **encryption scheme as corresponding to the second hash value in the second encryption table**.

58. (currently amended) An apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive ~~a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion~~ **an encrypted data segment**;

~~an encryption module adapted to decrypt each encrypted data segment;~~

a controller coupled to said input buffer ~~and said decryption module~~, said controller being adapted to **generate a first hash value from a first portion of the data segment and to dynamically** select a ~~set of encryption information for a current encrypted data segment to be decrypted based on data contained in a predetermined portion of the current encrypted data segment~~ **first encryption scheme from a plurality of encryption schemes, each encryption scheme comprising an encryption algorithm and an encryption key, and the first encryption scheme corresponding to the first hash value**;

a decryption module coupled to the controller and configured to utilize a computer processor to decrypt a second portion of the encrypted data segment using the first encryption scheme; and

an output buffer coupled to ~~said controller and~~ said decryption module, said output buffer being adapted to output decrypted data ~~including a plurality of decrypted data segments~~ **corresponding to the encrypted data segment**.

59. (currently amended) The apparatus of claim 58, wherein said decryption module comprises:

a plurality of decryption engines, each decryption engine corresponding to a ~~respective encryption algorithm different from each other~~ **a distinct encryption algorithm**.

60. (currently amended) The apparatus of claim ~~58~~ **59**, wherein said decryption module further comprises:

a data buffer coupled to each of the plurality of decryption engines.

61. (currently amended) The apparatus of claim ~~58~~ **59**, wherein said controller comprises:

~~a data selector adapted to select a predetermined portion of each encrypted data segment;~~

~~a decryption selector coupled with said data selector, adapted to select a set of decryption information in accordance with data contained in the predetermined portion,~~

~~the set of decryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter; and~~

a decryption controller adapted to select and activate a decryption engine **for encrypting the second portion of the data segment** based on the ~~encryption information~~ **first encryption scheme corresponding to the first hash value**.

Claims 62-63. (canceled)

64. (currently amended) The apparatus of claim ~~62~~ **58**, ~~wherein said decryption~~ **the** controller ~~comprises~~ **comprising** an encryption table ~~containing~~ **for selecting an encryption scheme from a hash value, the encryption table comprising**:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a ~~generated~~ **potential hash** value **corresponding to the first portion of the data encrypted segment**.

65. (canceled)

66. (currently amended) The apparatus of claim ~~65~~ **58**, ~~wherein the plurality of data segments are data packets in a data stream~~ **the input buffer being further configured to receive a data stream comprising a plurality of data packets, the encrypted data segment being at least one of the data packets**..

67. (currently amended) The apparatus of claim 66, ~~wherein~~ the first ~~predetermined~~ portion ~~contains~~ **of the encrypted data segment comprising** data for a first protocol layer, and the second ~~predetermined~~ portion ~~contains~~ **comprising** data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

68. (currently amended) The apparatus of claim ~~66~~ **67**, ~~wherein~~ the first ~~predetermined~~ portion ~~is~~ **of the encrypted data segment being** an Internet Protocol (IP) header ~~of the data packet~~.

69. (currently amended) The apparatus of claim 68, ~~wherein~~ the second ~~predetermined~~ portion ~~is either~~ **of the encrypted data segment being** one of:

a selected portion of a data field of the data packet;

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

Claims 70-71. (canceled)

72. (currently amended) The method of claim 58, ~~wherein the plurality of data segments are sectors in a data storage device~~ **the input buffer being further configured to read the encrypted data segment from a sector of a data storage device**.

73. (currently amended) The apparatus of claim 72, ~~wherein~~ the first ~~predetermined~~ portion ~~is~~ **of the encrypted data segment being** a first selected portion in ~~[[a]]~~ **the** sector ~~in a~~ **of the** data storage device, and the second ~~predetermined~~ portion ~~is~~ **being** a second selected portion ~~in~~ **of** the sector.

74. (currently amended) The apparatus of claim ~~58~~ **112**, ~~wherein said~~ **the** controller ~~comprises~~ **further comprising**:

a first encryption table for **mapping a plurality of potential hash values to the plurality of encryption schemes, wherein the controller identifies** ~~selecting~~ the first ~~set of decryption information based on data contained in the first predetermined portion~~ **encryption scheme as corresponding to the first hash value in the first encryption table**; and

a second encryption table for **mapping a plurality of potential hash values to the plurality of encryption schemes, wherein the controller identifies** ~~selecting~~ the second ~~set of decryption information based on data contained in the second predetermined portion~~ **encryption scheme as corresponding to the second hash value in the second encryption table**.

Claims 75-97. (canceled)

98. (new) A computer-implemented method for cryptographically processing data, the method comprising:

receiving a data segment;

selecting an unencrypted first portion, an unencrypted second portion, and an unencrypted third portion of the data segment;

generating a first hash value from the unencrypted first portion of the data segment;

associating each of a plurality of potential hash values with a corresponding encryption scheme belonging to a plurality of encryption schemes;

identifying a first encryption scheme of the plurality of encryption schemes, the first encryption scheme corresponding to a potential hash value that matches the first hash value;

encrypting, with a computer processor, the unencrypted second portion of the data segment to provide an encrypted second portion by applying the first encryption scheme;

generating a second hash value from the unencrypted second portion of the data segment;

identifying a second encryption scheme of the plurality of encryption schemes, the second encryption scheme corresponding to a potential hash value that matches the second hash value;

encrypting the unencrypted third portion of the data segment to provide an encrypted third portion by applying the second encryption scheme; and

outputting an encrypted data segment corresponding to the data segment, the encrypted data segment comprising the unencrypted first portion, the encrypted second portion, and the encrypted third portion of the data segment.

99. (new) The method of claim 98, the unencrypted first portion of the data segment being data corresponding to an internet protocol header of the data segment.

100. (new) The method of claim 98, further comprising:

identifying the first encryption scheme from the first unencrypted portion of the encrypted data segment;

recovering the unencrypted second portion by decrypting the encrypted second portion according to the first encryption scheme;

identifying the second encryption scheme from the unencrypted second portion of the encrypted data segment; and

recovering the unencrypted second portion by decrypting the encrypted second portion according to the second encryption scheme.

101. (new) A computer-implemented method for cryptographically processing data, the method comprising:

receiving an encrypted data segment comprising an unencrypted first portion, an encrypted second portion, and an encrypted third portion;

generating a first hash value from the unencrypted first portion of the encrypted data segment;

associating each of a plurality of potential hash values with a corresponding encryption scheme belonging to a plurality of encryption schemes;

identifying a first encryption scheme of the plurality of encryption schemes, the first encryption scheme corresponding to a potential hash value that matches the first hash value;

decrypting, with a computer processor, the encrypted second portion of the encrypted data segment to provide an unencrypted second portion by applying the first encryption scheme;

generating a second hash value from the unencrypted second portion of the data segment;

identifying a second encryption scheme of the plurality of encryption schemes, the second encryption scheme corresponding to a potential hash value that matches the second hash value;

decrypting the encrypted third portion of the data segment to provide an unencrypted third portion by applying the second encryption scheme; and

outputting an decrypted data segment corresponding to the encrypted data segment, the decrypted data segment comprising the unencrypted first portion, the unencrypted second portion, and the unencrypted third portion.

102. (new) The method of claim 101, the unencrypted first portion of the data segment being data corresponding to an internet protocol header of the encrypted data segment.

103. (new) The method of claim 1, further comprising:

generating a second hash value from the second portion of the first data segment;

identifying a second encryption scheme from among the plurality of encryption schemes, the second encryption scheme being identified by the second hash value corresponding to the second portion of the first data segment; and

encrypting a third portion of the first data segment using the second encryption scheme;

wherein the second portion of the first data segment is encrypted with the first encryption scheme identified by the first hash value corresponding to the first portion of the first data segment.

104. (new) The method of claim 1, wherein identifying a first encryption scheme from among the plurality of encryption schemes comprises:

locating the first hash value in an encryption table configured to map a plurality of values to a plurality of encryption schemes; and

identifying the first encryption scheme as corresponding to the first hash value in the encryption table.

105. (new) The method of claim 1, further comprising:

receiving a plurality of additional data segments; and

encrypting the plurality of additional data segments using a plurality of encryption schemes identified by hash values corresponding to portions of the plurality of additional data segments.

106. (new) The method of claim 25, further comprising:

generating a second hash value from the second portion of the first encrypted data segment;

identifying a second encryption scheme from among the plurality of encryption schemes, the second encryption scheme being identified by the second hash value corresponding to the second portion of the first encrypted data segment; and

decrypting a third portion of the first encrypted data segment using the second encryption scheme;

wherein the second portion of the first data segment is decrypted with the first encryption scheme identified by the first hash value corresponding to the first portion of the first encrypted data segment.

107. (new) The method of claim 25, wherein identifying a first encryption scheme from among the plurality of encryption schemes comprises:

locating the first hash value in an encryption table configured to map a plurality of values to a plurality of encryption schemes; and

identifying the first encryption scheme as corresponding to the first hash value in the encryption table.

108. (new) The method of claim 25, further comprising:

receiving a plurality of additional data segments; and

decrypting the plurality of additional data segments using a plurality of encryption schemes identified by hash values corresponding to portions of the plurality of additional data segments.

109. (new) The apparatus of claim 40, the controller being further configured to:

generate a second hash value from the second portion of the data segment; and

dynamically select a second encryption scheme from the plurality of encryption schemes, the second encryption scheme corresponding to the second hash value; and

the encryption module being further configured to:

encrypt a third portion of the data segment using the second encryption scheme.

110. (new) The apparatus of claim 40, the controller being configured to select the first encryption scheme from the plurality of encryption schemes by:

locating the first hash value in an encryption table configured to map a plurality of values to a plurality of encryption schemes; and

identifying the first encryption scheme as corresponding to the first hash value in the encryption table.

111. (new) The apparatus of claim 40, the input buffer being further configured to receive a plurality of additional data segments, and the encryption module being further configured to encrypt the plurality of additional data segments using a plurality of encryption schemes identified by hash values corresponding to portions of the plurality of additional data segments.

112. (new) The apparatus of claim 58, the controller being further configured to:

generate a second hash value from the second portion of the data segment; and

dynamically select a second encryption scheme from the plurality of encryption schemes, the second encryption scheme corresponding to the second hash value; and

the decryption module being further configured to:

decrypt a third portion of the data segment using the second encryption scheme.

113. (new) The apparatus of claim 58, the controller being configured to select the first encryption scheme from the plurality of encryption schemes by:

locating the first hash value in an encryption table configured to map a plurality of values to a plurality of encryption schemes; and

identifying the first encryption scheme as corresponding to the first hash value in the encryption table.

114. (new) The apparatus of claim 58, the input buffer being further configured to receive a plurality of additional data segments, and the decryption module being further configured to decrypt the plurality of additional data segments using a plurality of encryption schemes identified by hash values corresponding to portions of the plurality of additional data segments.